METHOD FOR ACCESS CONTROL IN DIGITAL PAY TELEVISION

DESCRIPTION

TECHNICAL FIELD

The present invention relates to a method for access control in the field of digital pay television.

DESCRIPTION OF THE PRIOR ART

The techniques used in pay television are based on two independent mechanisms: on the one hand on a scrambling/encryption of the video and/or audio signals, on the other hand on a function of commercial entitlements that are transmitted as secure messages to a descrambling module (with control access). The encryption may be applied easily on a digital bit stream. All the bits may be encrypted by using for example a block encryption. The scrambling is used for analog transmissions. By using such a scrambling method, the signal format is changed, the synchronization signals are deleted and transmitted separately in an encrypted form. The audio signal may be converted into a digital signal then encrypted. The encrypted digital audio signal may be inserted in the video signal.

The transmitted data are scrambled or encrypted by using a control word (CW) or a key. The control word or the key change after a short period. To send new keys to the subscriber receiving station, entitlement control messages (ECM) and entitlement management messages (EMM) are used.

These two messages, ECM and EMM, may be sent via the subscriber receiving station to a smart card.

The ECM messages contain information which allows the subscriber receiving station to descramble the video and/or audio signals. The descrambling data are returned to the latter in a form which allows the descrambling only if the user is authorized to access the current television program. When a user is represented by a smart card, the access authorization is indicated by entitlement data stored in the card.

The EMM messages contain information which can be used to update the user entitlement data, for example by modifying the data stored in the smart card.

The ECM and EMM messages have a digital signature field which ensures the integrity of the message (for example a Hash code). This prevents the users from being able to modify the content of their messages.

An ECM message is transmitted with the transmitted scrambled signal. It comprises three fields. The first field contains the access parameters. These parameters define the conditions in which access to a television program is allowed. This field makes possible, for example, a parental assessment (an additional pin code is then required by the decoder) and a geographic masking (a film may not be available in all European countries). The second field contains a control word in encrypted form. The last field contains a data integrity check.

An EMM message usually contains four fields. Each EMM message begins with an address field to select a receiver or receivers. There are two address modes, one for an individual station and the other for a group of such stations. The second field contains an entitlement for a given user. The third field contains the service keys in encrypted form. The last field contains a data integrity check. The EMM messages may also be used to

send a command to the decoder. The transmission of EMM messages is usually the result of an explicit request from the user to the service provider. These messages are usually individual. The EMM messages are not transmitted synchronously with the television service to which they apply. They are transmitted in advance in order to allow an authorized user to access a given program. Any network may be used to transmit these EMM messages to the receiver: modem, mail or radio broadcast.

To increase the probability that an EMM message has been received by the user, to renew a subscription for example, the latter is sent several times. The EMM messages are thus organized cyclically according to a given period for transmission. The duration of such a period is the main parameter for determining the maximum waiting time to obtain an entitlement for a user who has disconnected his receiving station for a long time.

An article of prior art, entitled "Functional model of a conditional access system" (8301 EBU Review Technical, 1995, No. 266), describes a functional model of a conditional access system for a use in digital television. Such a conditional access system comprises a combination of scrambling and encryption to prevent any unauthorized reception, the scrambling making it possible to render the images, the sound and the data unintelligible, the encryption protecting the secret keys that have been transmitted with the scrambled signal in order to allow the descrambler to function. After descrambling, any fault on the images or the sound must be imperceptible, that is to say that this conditional access system must be transparent.

The generation, transmission and use of entitlement management messages (EMMs) by the subscriber

authorization system are illustrated in the single figure.

This subscriber authorization system (SAS) 10 and a control word (CW) generator 11 are connected to an operator transmission station 12, each via an encryption circuit 13 and 14.

This operator transmission station 12 receives image signals I, sound signals S and data signals D which travel successively through a multiplexer 15, a scrambler 16, a modulator 17 and a transmitter 18.

On receipt of the signals transmitted by said transmitter 18 or transmitted, for example, via a satellite 20, a subscriber receiving station 21, which comprises successively a receiver 22, a demodulator 23, a descrambler 24, a demultiplexer 25, delivers image signals I', sound signals S', and data signals D'.

A conditional access subsystem, for example a smart card 26, which comprises two decryption circuits 27 and 28 and a security processor 29 (secret keys) is connected to this subscriber receiving station 21.

Descrambling requires the possession of a descrambler, a decryption circuit and a current service key. Decryption requires the use of entitlement management messages (EMM) for the current program, which usually uses secret keys stored in the smart card 26.

In the field of digital television, an on-demand consumption mode may be offered to the subscribers. This consumption mode can be used to view a service, for example a film showing, in subscription mode with a showing reservation or an operation of the type "impulsive pay per view/pay per time".

But such a consumption mode cannot be used to make promotional offers directly to a subscriber, or even to authorize a service in a targeted manner, for example to see a given film during a certain time window, according to the profile of a determined subscriber, so as to target a certain section of a subscriber population, without having to send validation then devalidation entitlement management messages (EMM).

The object of the invention is to resolve such a problem by providing a new consumption mode making it possible to authorize a service in a targeted manner and remotely according to a determined subscriber profile, without placing any heavy constraint on the operator transmission station.

SUMMARY OF THE INVENTION

The present invention therefore proposes a method of controlling access, in digital pay television, to information contained in a signal received by a subscriber receiving station comprising steps:

- of transmitting two types of messages via this subscriber receiving station to a user device, first entitlement control messages containing information to allow this subscriber receiving station to decode the signal and to offer the subscribers an on-demand operating method, second entitlement management messages containing information to allow the updating of the user's entitlement data,
- of generating in the user device an access authorization signal to allow the decoding of said signal by the subscriber receiving station if the user is authorized to access the information contained in the latter,

characterized in that first entitlement control messages are transmitted having a programmable profile content making it possible to authorize at least one

service or one program during a certain time window according to the profile of a determined subscriber, in order to produce a certain interactivity between the content of these first messages and the content of the user device in terms of subscription for the subscriber.

The method of the invention advantageously makes it possible:

- to make promotional offers, with a reduction in the number of entitlement management messages (EMM) transmitted,
- to carry out a "profiling" (taking account of the subscriber profile) easily,
- to fight against system piracy.

This method makes it possible, specifically, to fight against a certain type of system piracy, which consists, for a given subscriber, at a determined moment, in requesting a maximal subscription offer then after receiving the validation entitlement management message (EMM), requesting the basic subscription while blocking the subsequent entitlement management messages (EMM), including in particular the EMM cancellation message.

BRIEF DESCRIPTION OF THE DRAWINGS

The single figure illustrates a digital television signal transceiver system of the prior art.

DETAILED DESCRIPTION OF PARTICULAR EMBODIMENTS

In the method of the invention, which operates in a system as illustrated in the figure, the entitlement control messages ECM have a programmable profile content, which is used to produce a certain interactivity between the content of such ECM messages

and the content of the smart card, in terms of subscription for the subscriber.

It is thus possible for subscribers who benefit from a first offer O1 and a second offer O2, to be able to benefit from a third offer O3 under the control of the ECM messages, during the duration of a film for example. If it is then desired to no longer make such a promotional offer, the condition of the ECM messages is withdrawn.

Such a feature allows a viewing of certain services according to the profile of the subscribers, without having to first send a large number of entitlement management messages EMM.

It also makes it possible to ensure that the subscribers having a certain profile benefit from a reduced price. For example, a subscriber having paid for the entitlements for programs P1 and P2 and a commercial offer O1 may pay for a program for sale with two tokens, whereas the other users have to pay four tokens.

Such a feature also makes it possible to fight against system piracy. According to the method of the invention, a daily temporary offer is allocated for each service or each program. When a subscriber requests access to a program, for example a film showing, rather than give him access to a permanent offer, he is given access to a temporary offer.

Thus, if, after a short time, for example the same day, this subscriber requests a maximal subscription offer then changes his mind and, in order not to pay, requests the basic subscription, usually he is sent a cancellation entitlement management message EMM. If the latter then uses a "blocker" of these EMM messages, to

block the latter, he may then continue to have access to the requested service or to the requested program free of charge for two months for example.

On the other hand, with the method of the invention, since the offer is temporary, the next day, for example, the subscriber no longer has access to the service, or to the program, even though he has used an "EMM blocker". For subscribers having requested and confirmed their maximal offer, it is however necessary to send an EMM cancellation message with the permanent offer of this service, or of this program.

Exemplary embodiment of the method of the invention

. with conditional contents

Such conditional contents of EMM messages make it possible to work by using AND, OR, IF, ELSE and NOT functions, on the bitmap fields that the geographic address and/or subscription address represent. They also make it possible to produce a conditional operation between program numbers, for example a purchase of one program if another program has already been purchased.

Such a conditional operating mode appears in the form of a sequence, for example:

IF (offer O1) AND (offer O2) AND (NOT offer O3)

- Purchase program P1 in "Impulsive pay per view" mode offered for 50 tokens.
ELSE
- Purchase program P1 in "Impulsive pay per view" mode offered for 70 tokens.
ENDIF

. with conditional bitmaps

Conditional mechanisms can be used to offer a subscriber additional purchase or viewing possibilities, for example:

IF (((offer O1) AND ((offer O3) OR (offer O4))) OR (offer O2)
viewing of a program possible
ENDIF.

. with fight against system piracy

Conditional mechanisms can be used to fight against the aforementioned type of piracy, for example:

- on day to
IF ((temporary offer O5) OR (permanent offer O1))
- viewing of a program possible
ENDIF

- on day to + 1
IF ((temporary offer O6) OR (permanent offer O1))
- viewing of this program possible
ENDIF.